McAfee Embedded Control

System integrity, change control, and policy compliance in one solution for integrated control systems

McAfee® Embedded Control for integrated control systems (ICS)—a part of the Intel® Security product offering—maintains the integrity of your system by only allowing authorized code to run and only authorized changes to be made. It automatically creates a dynamic whitelist of the "authorized code" on the embedded system. Once the whitelist is created and enabled, the system is locked down to the known good baseline, no program or code outside the authorized set can run, and no unauthorized changes can be made. McAfee Integrity Control—which combines McAfee Embedded Control and the McAfee ePolicy Orchestrator® (McAfee ePO™) console—provides integrated audit and compliance reports to help you satisfy multiple compliance regulations.

Key Advantages

- Minimize your security risk by controlling what runs on your embedded devices and protecting the memory in those devices.
- Give access, retain control, reduce support costs.
- Selective enforcement.
- Deploy and forget.
- Make your devices compliance and audit ready.
- Real-time visibility.
- Comprehensive audit.
- Searchable change archive.
- Closed-loop reconciliation.

McAfee Embedded Control is a small-footprint, low-overhead, application-independent solution that provides "deploy-and-forget" security on embedded systems. By converting a system built on a commercial operating system into a "black box" with the characteristics of a closed, proprietary operating system, it prevents any unauthorized program from executing and making any unauthorized changes to the system. McAfee provides the required availability of the mission's operations in distributed control system environments. In addition, it provides the security foundations for critical infrastructure, discrete and process manufacturing environments, and smart grid deployments.

Assured System Integrity

Executional control

With McAfee Embedded Control, only programs contained in the McAfee dynamic whitelist are allowed to execute. All other programs are considered unauthorized. Their execution is prevented and the failure is logged by default. This prevents worms, viruses, spyware, and other malware that install themselves from executing illegitimately.

Memory control

Memory control ensures that running processes are protected from malicious attempts to hijack them. Unauthorized code injected into a running process is trapped, halted, and logged. Attempts to gain control of a system through buffer overflow, heap overflow, stack execution, and similar exploits are rendered ineffective and logged.[1]

Change Control

McAfee Embedded Control detects changes in real time. It provides visibility into the source of change, and verifies that changes were deployed onto the correct target systems, provides an audit trail of all changes, and allows changes to be made only through authorized means.

Out-of-box security
Protect against existing and zero-day threats.

Enable software change control
Enforce system manufacturer software change policies and ensure that only authorized software gets installed on in-field systems.

Reduced support costs
Reduce in-field breakage by preventing unauthorized changes and locking remote systems.

Control patching
Gain sufficient time to test patches by eliminating the need for emergency patching to stay secure.

Low touch
Work with it out of the box with minimal training required.

Compliance ready
Generate audit logs of every authorized change or unauthorized attempt.

Integration ready
Integrate with channel or retailer's manufacturing, provisioning, monitoring, change management, and in-field maintenance processes.

McAfee Embedded Control allows you to enforce change control processes by specifying the authorized means of making changes. You may control who can apply changes, which certificates are required to allow changes, what may be changed, and when changes can be applied.

Audit and Policy Compliance

McAfee Integrity Control provides dashboards and reports that help you meet compliance requirements. These are generated through the McAfee ePO console, which provides a web-based interface for users and administrators.

McAfee Embedded Control delivers integrated, closed-loop, real-time compliance and audit, complete with a tamperproof system of record for the authorized activity and unauthorized attempts.

McAfee GTI Integration: The Smart Way to Deal with Global Threats for Air-Gap Environments

McAfee Global Threat Intelligence (McAfee GTI) is an exclusive McAfee technology that tracks the reputation of files, messages, and senders in real time using millions of sensors worldwide. This feature uses cloud-based knowledge to determine the reputation of all files in your computing environment, classifying them as good, bad, and unknown. With McAfee GTI integration, you'll know with certainty when any malware has been inadvertently whitelisted. The GTI reputation is accessible in Internet connected as well as isolated McAfee ePO software environments.

ICS Industrial Controls—Threats Proven, Protection Needed

The unfortunate reality is that industrial controls, which are essential to the effective management of every type of distributed control system, are high-value targets for theft-of-service attacks and extortion, with potentially devastating consequences for production and distribution processes.

A 2010 CSIS study found that cyberattacks on critical infrastructure are widespread, with the cost of downtime as a result of these attacks averaging US $6 million per day.[2] The increasing success of attackers can be attributed to the technical characteristics of many of these systems, including:

- Lack of security controls for embedded devices.
- Unpatchable or outdated control systems.
- Weak or non-existent passwords.
- Malware injections from less to more critical network segments.
- Unprotected HMI and other databases.
- Buffer overflows and other threats in control system applications.
- Modems with open ports.
- Inadequately secured wireless communications.
- Uncontrolled remote access or backdoors.

Too often, there is a disconnect between the importance of these assets, their vulnerabilities, and the security budget. Since the CSIS study, Operation Aurora has impacted the supply chain of critical and non-critical infrastructure; Richard Clark's exposé, *Cyber War: The Next Threat to National Security and What to Do About It*, built the case that attackers are backed by nation states and becoming swiftly educated; and Stuxnet became the first substantive and direct threat to control systems. It appears that potential enemies are gaining knowledge about proprietary control systems as potential targets of extortion, intellectual property theft, and theft of service, all at a time when associated budgets for security are being reduced.[3]

Against this backdrop, the manufacturers, designers, and users of ICS recognize that they must prioritize availability above all else. As a result, the evolution of ICS (both SCADA and DCS) allows greater connectivity to IP networks for WAN communications; greater connectivity to corporate IT infrastructures, where threats tend to be more pervasive due to high rates of IP connectivity and users; and greater remote access to the control systems environment. Somewhat counterintuitively, the net effect is that these systems become more vulnerable and sensitive to use of security technologies, which may interrupt services.

In 2008, McAfee launched the Initiative to Fight Cybercrime, which includes critical infrastructure protection. This initiative has three main focus areas: Research and innovation, education and awareness, and legislation and policy assistance. Through this initiative, McAfee is helping critical infrastructure industries and governments around the world understand the threat landscape, develop mitigation strategies, and establish policies to help ensure an effective approach to the problem.

The Global Smart Grid seeks to address these threats while helping to ensure end-to-end security and privacy of information. To address current security threats, effective solutions need to be embedded in distributed control systems environments with operational integrity as the primary goal. These solutions must segregate control from IT, validate users and devices, and protect sensitive data while addressing the vulnerabilities that may exist in these systems.

Next Steps

For more information, visit **www.mcafee.com/embeddedsecurity** or contact your local McAfee representative.

About McAfee Embedded Security

McAfee Embedded Security solutions help manufacturers ensure that their products and devices are protected from cyberthreats and attacks. McAfee solutions span a wide range of technologies, including application whitelisting, antivirus and anti-malware protection, device management, encryption, and risk and compliance—and all leverage the industry-leading McAfee Global Threat Intelligence. Our solutions can be tailored to meet the specific design requirements for a manufacturer's device and its architectures.

Feature	Description	Benefit
	Guaranteed System Integrity	
External threat defense	Ensures that only authorized code can run. Unauthorized code cannot be injected into memory. Authorized code cannot be tampered with.	• Eliminates emergency patching, reduces number and frequency of patching cycles, enables more testing before patching, reduces security risk for difficult-to-patch systems. • Reduces security risk from zero-day, polymorphic attacks via malware such as worms, viruses, and Trojans and code injections like buffer-overflow, heap-overflow, and stack-overflow. • Maintains integrity of authorized files, ensuring the system in production is in a known and verified state. • Reduces cost of operations via both planned patching and unplanned recovery downtime and improves system availability.
Internal threat defense	Local administrator lockdown gives the flexibility to disable even administrators from changing what is authorized to run on a protected system, unless presented by an authentic key.	• Protects against internal threat. • Locks down what runs on embedded systems in production and prevents change even by administrators.

(continued)

Advanced Change Control		
Secure authorized updates by manufacturer	Ensures that only authorized updates can be implemented on in-field embedded systems.	• Ensures that no out-of-band changes can be deployed on systems in the field. Prevents unauthorized system changes before they result in downtime and generate support calls. • Manufacturers can choose to retain control over all changes themselves, or authorize only trusted customer agents to control changes.
Verify that changes occurred within approved window	Ensure that changes were not deployed outside of authorized change windows.	• Prevent unauthorized change during fiscally sensitive time windows or during peak business hours to avoid operational disruption and/or compliance violations.
Authorized updaters	Ensure that only authorized updaters (people or processes) can implement changes on production systems.	• Ensure that no out-of-band changes can be deployed on production systems.
Real-Time, Closed-Loop Audit and Compliance		
Real-time change tracking	Track changes as soon as they happen across the enterprise.	• Ensure that no out-of-band changes can be deployed on production systems.
Comprehensive audit	Capture complete change information for every system change: Who, what, where, when, and how.	• An accurate, complete, and definitive record of all system changes.
Identify sources of change	Link every change to its source: Who made the change, the sequence of events that led to it, the process/program that affected it.	• Validate approved changes, quickly identify unapproved changes, and increase change success rate.
Low Operational Overhead		
Deploy and forget	Software installs in minutes, no initial configuration or setup necessary. No ongoing configuration necessary.	• Works out of the box. Effective immediately after installation. Does not have any ongoing maintenance overhead, thereby a favorable choice for a low operating expense (OPEX) security solution configuration.
Rules-free, signature-free, no learning period, application independent	Does not depend on rules or signature databases and is effective across all applications immediately with no learning period.	• Needs very low attention from an administrator during server lifecycle. • Protects server until patched or unpatched server with low ongoing OPEX. • Its effectiveness does not depend on quality of any rules or policies.
Small footprint, low runtime overhead	Takes up less than 20 MB disk space. Does not interfere with application's runtime performance.	• Ready to be deployed on any mission-critical production system without impacting its run-time performance or storage requirements.
Guaranteed no false positives or false negatives	Only unauthorized activity is logged.	• Accuracy of results reduces OPEX as compared to other host intrusion prevention solutions by dramatically reducing the time needed to analyze logs daily/weekly. • Improves administrator efficiency, reduces OPEX.

1. Only available on Microsoft Windows platforms
2. In the Crossfire, Center for Strategic and International Studies, January 2010
3. Ibid.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com

60744ds_embedded-control-ics_1213B